



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/636,102	08/10/2000	Daniel O. Ramos	60259	6353
23735	7590	03/24/2005	EXAMINER	
DIGIMARC CORPORATION 9405 SW GEMINI DRIVE BEAVERTON, OR 97008			VU, THANH T	
			ART UNIT	PAPER NUMBER
			2174	

DATE MAILED: 03/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.



UNITED STATES PATENT AND TRADEMARK OFFICE

RECEIVED

MAR 24 2005

Technology Center 2100

COMMISSIONER FOR PATENTS  
UNITED STATES PATENT AND TRADEMARK OFFICE  
P.O. Box 1450  
ALEXANDRIA, VA 22313-1450  
www.uspto.gov

**BEFORE THE BOARD OF PATENT APPEALS  
AND INTERFERENCES**

Application Number: 09/636,102  
Filing Date: August 10, 2000  
Appellant(s): RAMOS ET AL.

DIGIMARC CORPORATION  
For Appellant

**EXAMINER'S ANSWER**

This is in response to the appeal brief filed 08/23/2004.

**(1) *Real Party in Interest***

A statement identifying the real party in interest is contained in the brief.

**(2) *Related Appeals and Interferences***

The brief does not contain a statement identifying the related appeals and interferences which will directly affect or be directly affected by or have a bearing on the decision in the

pending appeal is contained in the brief. Therefore, it is presumed that there are none. The Board, however, may exercise its discretion to require an explicit statement as to the existence of any related appeals and interferences.

**(3) Status of Claims**

The statement of the status of the claims contained in the brief is correct.

**(4) Status of Amendments After Final**

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

**(5) Summary of Invention**

The summary of invention contained in the brief is correct.

**(6) Issues**

The appellant's statement of the issues in the brief is correct.

**(7) Grouping of Claims**

Appellant's brief includes a statement that claims 2, 5-7, 9 and 14-20 do not stand or fall together and provides reasons as set forth in 37 CFR 1.192(c)(7) and (c)(8).

**(8) Claims Appealed**

The copy of the appealed claims contained in the Appendix to the brief is correct.

**(9) Prior Art of Record**

5606609	Houser et al.	02-1997
5801689	Huntsman	09-1998

**(10) Grounds of Rejection**

The following ground(s) of rejection are applicable to the appealed claims:

Claims 2, 5-7, 9-10 and 14-20 are rejected under 35 U.S.C. 102(e) as being anticipated by Houser et al. ("Houser", U.S. Pat. No. 5,606,609).

Per claim 2, Houser teaches a file browser system comprising:

a file browser for displaying in a user interface a representation of media object files stored in memory (fig. 4B; col. 11, lines 11-34); and

a file browser extension for decoding an object identifier from a selected media object file (fig. 8; decryptor 820; col. 15, lines 19-20 and lines 61-67) and for displaying in an extension of the user interface metadata or an action associated with the media object file via the object identifier (col. 16, lines 34-50; col. 17, lines 5-12) wherein the object identifier is decoded from a watermark embedded in the selected media object file (col. 4, lines 3-10; col. 7, lines 30-43; col. 15, lines 19-20 and lines 61-67; The examiner considers a watermark as a security object being embedded in a electronic document, see col. 7, lines 30-43 and col. 12, lines 30-35).

Per claim 5, Houser teaches a file browser system comprising:

a file browser for displaying in a user interface a representation of media object files stored in memory (fig. 4B; col. 11, lines 11-34); and

a file browser extension for decoding an object identifier from a selected media object file and (fig. 8; decryptor 820; col. 15, lines 19-20 and lines 61-67) for displaying in an extension of the user interface metadata or an action associated with the media object file via the object identifier (col. 16, lines 34-50; col. 17, lines 5-12); wherein the file browser extension forwards the object identifier to a metadata server (col. 16, lines 1-9) and displays metadata or an action returned from the server (col. 16, lines 34-50; col. 17, lines 5-12).

Per claim 6, Houser teaches the file browser system of claim 5 wherein the file browser extension extracts and displays metadata from the media object file along with metadata returned from the metadata server (col. 16, lines 34-50 and col. 17, lines 5-12).

Per claim 7, Houser teaches a file browser system comprising: a file browser for displaying in a user interface a representation of media object files stored in memory (fig. 4B; col. 11, lines 11-34); and

a file browser extension for decoding an object identifier from a selected media object file (fig. 8; decryptor 820; col. 15, lines 19-20 and lines 61-67) and for displaying in an extension of the user interface metadata or an action associated with the media object file via the object identifier (col. 16, lines 34-50 and col. 17, lines 5-12); wherein the metadata or action is displayed as a URL link to information or a program associated with the selected media object file (col. 16, lines 34-50 and col. 17, lines 5-12 and lines 33-48).

Per claim 9, Houser teaches a file browser system comprising:

a file browser for displaying in a user interface media object files stored in memory (fig. 4B; col. 11, lines 11-34); and

a file browser extension for encoding an object identifier into a selected media object file (fig. 6; encryptor 620; col. 4, lines 3-10; col. 14, lines 38-50) and for displaying in an extension of the user interface one or more options for enabling a user to enter input to control the encoding of the object identifier (col. 13, lines 35-65); wherein the file browser extension comprises a watermark encoder for encoding the object identifier into the selected media object file (col. 7, lines 30-43; col. 11, lines 15-25; The examiner considers a watermark as a security object being embedded in a electronic document, see col. 7, lines 30-43 and col. 12, lines 30-35.)

Per claim 10, Houser teaches a watermark decoder system comprising:

a host application having a user interface for displaying a representation of media object files (fig. 4B; col. 11, lines 11-34); and

an extension to the host application for decoding a watermark from a selected media object file (fig. 8; decryptor 820; col. 15, lines 19-20 and lines 61-67) and for displaying in an extension of the user interface metadata or an action associated with the media object file via the watermark (col. 16, lines 34-50; and col. 17, lines 5-12).

Per claim 14, Houser teaches a method of rendering a media object comprising:

decoding an object identifier from the media object (fig. 8; decryptor 820; col. 15, lines 19-20 and lines 61-67);

sending the object identifier to a metadata server (fig. 8; col. 15, lines 15-27; col. 16, lines 1-9);

receiving a brand identifier from the metadata server (col. 7, lines 45-60; col. 10, lines 23-27); and

displaying a representation of the brand identifier (col. 16, lines 34-50; col. 17, lines 5-12).

Per claim 15, Houser teaches the method of claim 14 wherein the object identifier is decoded from a watermark embedded in the media object (fig. 8; decryptor 820; col. 4, lines 3-10; col. 15, lines 19-20 and lines 61-67; col. 16, lines 52-67).

Per claim 16, Houser teaches the method of claim 14 wherein the media object is a video or an image, and the representation of the brand identifier is a graphic superimposed on a

Art Unit: 2174

rendering of the video or image (col. 7, lines 45-60; col. 10, lines 23-27; col. 16, lines 34-50; col. 17, lines 5-13).

Per claim 17, Houser teaches the method of claim 16 wherein the graphic is a hot link to information or an action associated with the media object (col. 7, lines 45-60; col. 10, lines 23-27; col. 16, lines 34-50; col. 17, lines 5-13).

Per claim 18, Houser teaches the method of claim 17 wherein selecting the hot link causes retrieval of the information or action from a remote server (col. 8, lines 58-65; col. 9, lines 55-60).

Per claim 19, Houser teaches a method for extending a user interface of a media player comprising:

in response to input requesting playback of a media object, extracting an object identifier from the media object (fig. 8; decryptor 820; col. 11, lines 52-61; col. 15, lines 19-20 and lines 61-67);

using the object identifier to look up metadata associated with the media object (fig. 8; col. 15, lines 45-67);

extending a user interface of a media player to include a representation of the metadata associated with the media object (col. 16, lines 34-45; col. 15, lines 34-50).

Per claim 20, Houser teaches the method of claim 19 wherein extracting the object identifier includes decoding the object identifier from a watermark embedded in the media object (fig. 8; col. 4, lines 3-10; col. 15, lines 19-20 and lines 61-67; The examiner considers a watermark as a security object being embedded in a electronic document, see col. 7, lines 30-43 and col. 12, lines 30-35).

Claims 11-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over (“Houser”, U.S. Pat. No. 5,606,609) in view of Huntsman (U.S. Pat. No. 5,801,689).

Per claim 11, Houser teaches a browser on a computer readable medium, the browser comprising: a listener program for identifying a media object in a document (fig. 8; interpreter module 250; col. 15, lines 25-27); and for inserting a handler into the document when an object identifier is extracted from the media object (col. 16, lines 34-50 and lines 52-67); wherein the handler is operable to display metadata linked via the object identifier in response to user input (col. 13, lines 35-50; col. 16, lines 34-50; col. 17, lines 5-12 and lines 33-48), but does not teach the browser is an internet browser having an HTML document. However, Huntsman teaches an Internet browser having an HTML document (col. 4, lines 1-20). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to include the teaching of Huntsman in the invention of Houser in order to provide a means for accessing the document information from a remote location.

Per claim 12, Houser teaches the internet browser of claim 11 wherein the object identifier is decoded from a watermark embedded in the media object (fig. 8; decryptor 820; col. 15, lines 19-20 and lines 61-67).

Per claim 13, Houser teaches the internet browser of claim 11 wherein the metadata is retrieved from a metadata server by sending the object identifier to the metadata server (*fig. 8; col. 16, lines 34-50; col. 17, lines 5-12; the security object information is being forwarded to the verification processor 830, which performs verification processing, see col. 16, lines 1-9*).

**(11) Response to Argument**



**Claim 1**, the Appellant argues that Houser does not teach “How to decode an object identifier from a watermark embedded in a selected media object file”. The Examiner does not agree because Houser teaches decoding an object identifier from a watermark embedded in a selected media object file (*col. 4, lines 3-10; col. 7, lines 30-43; col. 15, lines 19-20 and lines 61-67; The examiner interprets a watermark as a security object being embedded in a electronic document, see col. 7, lines 30-43 and col. 12, lines 30-35. It is noted that the interpretation of a watermark as a security object is consistent with the applicant’s definition of a watermark. Namely, a watermark is a machine-readable code that is embedded in media by modifying the media, see page 1, lines 22-25.*)

In addition, the Appellant also points out that the Examiner relies on a different portion of Houser in the Advisory Action in response to the Appellant’s amendment after final. It is noted that the Examiner relies on additional portions of Houser in order to clarify the Examiner’s position.

**Claim 5**, the Appellant argues that Houser does not teach “forwarding the object identifier to a metadata server and displays metadata or an action returned from the server. The Examiner does not agree because by definition, a server means a computer program that provides services to other computers programs (and their users) in the same or other computers ([www.whatis.com](http://www.whatis.com) and [www.netlingo.com](http://www.netlingo.com)). Houser teaches forwarding the object identifier to a metadata server (*fig. 8; the security object information is being forwarded to the verification processor 830, which performs verification processing, see col. 16, lines 1-9*) and displays metadata or an action returned from the server (*col. 16, lines 34-50; col. 17, lines 5-12*).

**Claim 6**, the Appellant argues that Houser does not teach “the file browser extension extracts and displays metadata from the media object file along with metadata returned from the metadata server”. The Examiner does not agree because Houser teaches the file browser extension extracts and displays metadata from the media object file along with metadata returned from the metadata server (*col. 15, lines 62-67; col. 16, lines 34-50 and col. 17, lines 5-12*).

**Claim 7**, the Appellant argues that Houser does not teach that “the metadata or action is displayed as a URL link to information or a program associated with the selected media object file”. The Examiner does not agree because Houser reads on the claim language of the metadata or action is displayed as a program associated with the selected media object file (*col. 16, lines 34-50 and col. 17, lines 5-12 and lines 33-48*).

**Claim 9**, the Appellant argues that Houser does not teach “a watermark encoder for encoding the object identifier into the selected media object file”. The Examiner does not agree because Houser teaches a watermark encoder for encoding the object identifier into the selected media object file (*fig. 6; encryptor 620; col. 4, lines 3-10; col. 14, lines 38-50; col. 11, lines 15-25; The examiner considers a watermark as a security object being embedded in a electronic document, see col. 7, lines 30-43 and col. 12, lines 30-35. It is noted that the interpretation of a watermark as a security object is consistent with the applicant’s definition of a watermark. Namely, a watermark is a machine-readable code that is embedded in media by modifying the media, see page 1, lines 22-25*).

**Claim 10**, the Appellant argues that Houser does not teach “decoding a watermark from a selected media object file and for displaying in an extension of the user interface metadata or an action associated with the media object file via the watermark. The Examiner does not agree

because Houser teaches decoding a watermark from a selected media object file (*fig. 8; decryptor 820; col. 15, lines 19-20 and lines 61-6; The examiner considers a watermark as a security object being embedded in a electronic document, see col. 7, lines 30-43 and col. 12, lines 30-35. It is noted that the interpretation of a watermark as a security object is consistent with the applicant's definition of a watermark. Namely, a watermark is a machine-readable code that is embedded in media by modifying the media, see page 1, lines 22-25*) and for displaying in an extension of the user interface metadata or an action associated with the media object file via the watermark (*col. 16, lines 34-50; and col. 17, lines 5-12.*)

**Claim 11**, the Appellant argues that Houser does not teach “inserting a handler into the document when an object identifier is extracted from the media object wherein the handler is operable to display metadata linked via the object identifier in response to user input”. The Examiner does not agree because Houser teaches inserting a handler into the document when an object identifier is extracted from the media object (*col. 16, lines 34-50 and lines 52-67*); wherein the handler is operable to display metadata linked via the object identifier in response to user input (*col. 13, lines 35-50; col. 16, lines 34-50; col. 17, lines 5-12 and lines 33-48.*)

In addition, the Appellant also points out that the Examiner relies on a different portion of Houser in the Advisory Action. It is noted that the Examiner relies on additional portions of Houser in order to clarify the Examiner's position.

**Claim 12**, the Appellant argues that Houser does not teach, “the object identifier is decoded from a watermark embedded in the media object”. The Examiner does not agree because Houser teaches the object identifier is decoded from a watermark embedded in the media object (*fig. 8; decryptor 820; col. 15, lines 19-20 and lines 61-67; The examiner considers*

Art Unit: 2174

*a watermark as a security object being embedded in a electronic document, see col. 7, lines 30-43 and col. 12, lines 30-35.)*

**Claim 13**, the Appellant argues that Houser does not teach “the metadata is retrieved from a metadata server by sending the object identifier to the metadata server”. The Examiner does not agree because by definition, a server means a computer program that provides services to other computers programs (and their users) in the same or other computers ([www.whatis.com](http://www.whatis.com) and [www.netlingo.com](http://www.netlingo.com)). Therefore, Houser teaches the metadata is retrieved from a metadata server by sending the object identifier to the metadata server (*fig. 8; col. 16, lines 34-50; col. 17, lines 5-12; the security object information is being forwarded to the verification processor 830, which performs verification processing, see col. 16, lines 1-9.*)

**Claim 14**, the Appellant argues that Houser does not teach “sending the object identifier to a metadata server, receiving a brand identifier from the metadata server, and displaying a representation of the brand identifier”. The Examiner does not agree because by definition, a server means a computer program that provides services to other computers programs (and their users) in the same or other computers ([www.whatis.com](http://www.whatis.com) and [www.netlingo.com](http://www.netlingo.com)). Therefore, Houser reads on the claim language of sending the object identifier to a metadata server (*fig. 8; col. 15, lines 15-27; the security object information is being forwarded to the verification processor 830, which performs verification processing, see col. 16, lines 1-9*), receiving a brand identifier from the metadata server (col. 7, lines 45-60; col. 10, lines 23-27), and displaying a representation of the brand identifier (col. 16, lines 34-50; col. 17, lines 5-12).

**Claim 15**, the Appellant argues that Houser does not teach “the object identifier is decoded from a watermark embedded in the media object”. The Examiner does not agree

because Houser teaches the object identifier is decoded from a watermark embedded in the media object (*fig. 8; decryptor 820; col. 4, lines 3-10; col. 15, lines 19-20 and lines 61-67; col. 16, lines 52-67. The examiner considers a watermark as a security object being embedded in a electronic document, see col. 7, lines 30-43 and col. 12, lines 30-35. It is noted that the interpretation of a watermark as a security object is consistent with the applicant's definition of a watermark. Namely, a watermark is a machine-readable code that is embedded in media by modifying the media, see page 1, lines 22-25.*)

**Claim 16**, the Appellant argues that Houser does not teach “the media object is a video or an image, and the representation of the brand identifier is a graphic superimposed on a rendering of the video or image”. The Examiner does not agree because Houser teaches the media object is a video or an image, and the representation of the brand identifier is a graphic superimposed on a rendering of the video or image (*col. 7, lines 45-60; col. 10, lines 23-27; col. 16, lines 34-50; col. 17, lines 5-13.*)

**Claim 17**, the Appellant argues that Houser does not teach “the graphic is a hot link to information or an action associated with the media object”. The Examiner does not agree because Houser teaches the graphic is a hot link to information or an action associated with the media object (*col. 7, lines 45-60; col. 10, lines 23-27; col. 16, lines 34-50; col. 17, lines 5-13.*)

**Claim 18**, the Appellant argues that Houser does not teach “the hot link causes retrieval of the information or action from a remote server.” Houser teaches the hot link causes retrieval of the information or action from a remote server (*col. 8, lines 58-65; col. 9, lines 55-60.*)

**Claim 19**, the Appellant argues that Houser does not teach “extending a user interface of a media player to include a representation of the metadata associated with the media object.” The

Art Unit: 2174

Examiner does not agree because Houser teaches extending a user interface of a media player to include a representation of the metadata associated with the media object (*col. 11, lines 54-61; col. 16, lines 34-45; col. 15, lines 34-50.*)

**Claim 20**, the Appellant argues that Houser does not teach “extracting the object identifier includes decoding the object identifier from a watermark embedded in the media object.” The Examiner does not agree because Houser teaches extracting the object identifier includes decoding the object identifier from a watermark embedded in the media object (*fig. 8; col. 4, lines 3-10; col. 15, lines 19-20 and lines 61-67; The examiner considers a watermark as a security object being embedded in a electronic document, see col. 7, lines 30-43 and col. 12, lines 30-35 It is noted that the interpretation of a watermark as a security object is consistent with the applicant’s definition of a watermark. Namely, a watermark is a machine-readable code that is embedded in media by modifying the media, see page 1, lines 22-25.*)

Accordingly, the claimed invention as represented in the claim does not represent a patentable distinction over the prior art of record.

For the above reasons, it is believed that the rejections should be sustained.

Art Unit: 2174

Respectfully submitted,

*Kristine Kincaid*

KRISTINE KINCAID  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100

Thanh Vu  
March 18, 2005

Conferees  
Kristine L. Kincaid

Joseph H. Feild

*J. Feild*

DIGIMARC CORPORATION  
19801 SW 72ND AVENUE  
SUITE 100  
TUALATIN, OR 97062